



#2
BT
2161 03-19-02

Attorney Docket No.: BHT-3212-3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

Chia-Chi CHANG

Application No.: 10/028,820

Filed: December 28, 2001

:
:
: Group Art Unit: 2161
:
: Examiner: Not Yet Assigned
:
:

For: **SYSTEM AND METHOD FOR MANAGING AND SECURING TRANSACTION
INFORMATION VIA A THIRD PARTY**

CLAIM TO PRIORITY UNDER 35 U.S.C. § 119

Assistant Commissioner of Patents
Washington, D.C. 20231

Sir:

RECEIVED

MAR 15 2002

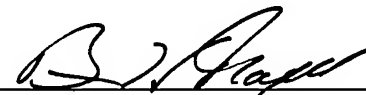
Technology Center 2100

Pursuant to the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55, Applicant
claims the right of priority based upon **Chinese Application No. 090127038** filed
October 31, 2001.

A certified copy of Applicant's priority document is submitted herewith.

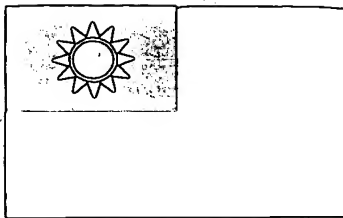
Respectfully submitted,

By:


Bruce H. Troxell
Reg. No. 26,592

TROXELL LAW OFFICE PLLC
5205 Leesburg Pike, Suite 1404
Falls Church, Virginia 22041
Telephone: (703) 575-2711
Telefax: (703) 575-2707

Date: March 13, 2002



中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，

其申請資料如下：

This is to certify that annexed is a true copy from the records of this office of the application as originally filed which is identified hereunder:

申請日：西元 2001 年 10 月 31 日

Application Date

10/028,820-CHANG

申請案號：090127038

Application No:

GAR 2161
BHT-3212-3

申請人：網元國際金流股份有限公司

Applicant(s)

RECEIVED

MAR 15 2002

Technology Center 2100

局長

Director General

陳明邦

發文日期：西元 2002 年 1 月 14 日

Issue Date

發文字號：

09111000624

Serial No.

申請日期：	案號：90127038
類別：	

(以上各欄由本局填註)

發明專利說明書

一、 發明名稱	中 文	經由第三方來管理及保全交易資訊之系統及方法
	英 文	SYSTEM AND METHOD FOR MANAGING AND SECURING TRANSACTION INFORMATION VIA A THIRD PARTY
二、 發明人	姓 名 (中文)	1. 張家齊
	姓 名 (英文)	1. Chang, Chia-Chi
	國 籍	1. 中華民國
	住、居所	1. 苗栗縣竹南鎮龍鳳里9鄰龍昇街51號
三、 申請人	姓 名 (名稱) (中文)	1. 網元國際金流股份有限公司
	姓 名 (名稱) (英文)	1. NetBuck Payment Service Co., Ltd.
	國 籍	1. 中華民國
	住、居所 (事務所)	1. 台北市光復南路495號4樓
	代表人 姓 名 (中文)	1. 羅鎮
	代表人 姓 名 (英文)	1. Lo, Attlee



四、中文發明摘要 (發明之名稱：經由第三方來管理及保全交易資訊之系統及方法)

本發明係提供一種經由一第三方來管理及保全一交易資訊之系統及方法。該交易資訊係關於一筆於一買方與一賣方之間所達成之交易。該交易資訊包含關於該賣方之一第一資訊以及關於該買方之一第二資訊。根據本發明之系統包含一第一處理裝置以及一第二處理裝置。該第一處理裝置係由該第三方所操控。該第二處理裝置係由該賣方所操控。該第一處理裝置係用以基於該第一資訊對該第二資訊加密以產生一加密的第二資訊，並且將該第一資訊以及該加密的第二資訊傳送出去。該第二處理裝置係用以儲存從該第一處理裝置傳送來之該第一資訊以及該加密的第二資訊。並且當該賣方要求對該交易做一核對時，該第二處理裝置係用以將該第一資訊以及該加密的第二資訊回傳至

英文發明摘要 (發明之名稱：SYSTEM AND METHOD FOR MANAGING AND SECURING TRANSACTION INFORMATION VIA A THIRD PARTY)



四、中文發明摘要 (發明之名稱：經由第三方來管理及保全交易資訊之系統及方法)

該第一處理裝置。當該第一處理裝置接收到回傳之該第一資訊以及該加密的第二資訊時，該第一處理裝置則基於該第一資訊對該加密的第二資訊解密進而重新獲得該交易資訊。該第一處理裝置隨後根據該重新獲得之交易資訊產生一回應資訊，並且隨後將該回應資訊傳送至該第二處理裝置，其中該回應資訊係回應該賣方對核對該交易之要求。藉此，該交易資訊可避免被該賣方所竄改。

英文發明摘要 (發明之名稱：SYSTEM AND METHOD FOR MANAGING AND SECURING TRANSACTION INFORMATION VIA A THIRD PARTY)



本案已向

國(地區)申請專利

申請日期

案號

主張優先權

無

有關微生物已寄存於

寄存日期

寄存號碼

無

五、發明說明 (1)

發明領域

本發明係關於一種管理及保全交易資訊之系統及方法，尤指一種經由第三方管理及保全交易資訊之系統及方法。

發明背景

隨著科技的進步，人類的生活習慣也不斷的改善，尤其在網際網路出現後，縮短了時間與空間，人與人之間的溝通方式已經邁入了一個新紀元。特別是在購物消費方面，網際網路更是帶給人類前所未有的便利性。在過去，如果人們想要買到一個符合自己標準、價格又便宜的商品，往往必須在各大街小巷中的各大小商店拼命尋找，才有機會找到，如果運氣不好的話，常常是費心費力卻又達不到目的地。由於網路的出現，現在的人們只需在一台電腦螢幕前，瀏覽世界各地的網站，就能找到自己心目中物美價廉的商品，而且還可以藉由物流服務提供者配送到家，幫人們省下不少購物時間，並且不需要出國即可擴大購物領域。

然而，網際網路雖然為人們帶來了便利的環境，卻也帶來了隱私性不足的問題。當一消費者於網際網路上消費向網路商家要求交易時，必須將其具私密性的一個人資訊，如帳號、密碼及信用卡號碼等，藉由網路傳輸，完全提供給網路商家，再由網路商家向發卡銀行取得授權，才能達成該筆交易。可是網路傳輸的資訊容易被不法人士截



五、發明說明 (2)

取，進而藉該個人資料從事非法的行為。而且，如果該消費者不幸遇到不肖的網路商家，該消費者也會面臨該個人資料遭到冒用的危險。

先前技術關於交易資訊的管理，於美國專利第5,915,022號專利中，即提出將交易資訊加密的方法，能使得不法人士即使截取到該交易資訊，卻無法將其解密，當然也就無法藉該交易資訊從事非法的行為。然而，該先前技術仍是由網路商家負責解密的工作，仍然無法防止不肖網路商家冒用消費者資訊的問題。

因此，本發明之一目的在於提供一種經由一第三方管理及保全交易資訊之系統及方法。藉由不涉及交易的公正第三方，參與該交易資訊的管理及保全，特別地，該交易資訊中關於買方(消費者)的個人資料之加、解密工作並非交由賣方(商家)執行，而是交由該第三方來執行。如此即可令不肖的網路商家無可趁之機，藉此確實地保護買方(消費者)的權益。

發明概述

本發明之一目的在於提供一種經由一第三方來管理及保全關於一筆交易之一交易資訊的系統及方法。該筆交易係於一買方與一賣方之間所達成。藉由該受信任的第三方參與該交易資訊的管理及保全。特別地，該交易資訊之管理及保全過程中，關於該買方(消費者)的相關資訊之加、解密工作並非交由該賣方執行，而是交由該第三方來執



五、發明說明 (3)

行。如此賣方(商家)無法獲知買方(消費者)的資訊，即便是不肖的網路商家也就無可趁之機，藉此確實地保護該消費者的權益。

根據本發明之一較佳具體實施例，一種資料處理系統係提供用來經由一第三方來管理及保全關於一交易之一交易資訊。該交易係於一買方與一賣方之間達成，該交易資訊包含關於該賣方之一第一資訊以及關於該買方之一第二資訊。該資料處理系統包含一第一處理裝置以及一第二處理裝置。該第一處理裝置係由該第三方所操控。該第二處理裝置係由該賣方所操控。該第一處理裝置係用以基於該第一資訊對該第二資訊加密以產生一加密的第二資訊，並且將該第一資訊以及該加密的第二資訊傳送至該第二處理裝置。該第二處理裝置係用以接收並儲存從該第一處理裝置傳送來之該第一資訊以及該加密的第二資訊。當該賣方要求對該交易做一核對時，該第二處理裝置係用以將該第一資訊以及該加密的第二資訊回傳至該第一處理裝置。於該第一處理裝置接收到回傳之該第一資訊以及該加密的第二資訊之後，該第一處理裝置隨即基於該第一資訊對該加密的第二資訊解密進而重新獲得該交易資訊。該第一處理裝置並且根據該重新獲得之交易資訊產生一回應資訊，該回應資訊係回應該賣方對核對該交易之要求。該第一處理裝置並且隨後將該回應資訊傳送至該第二處理裝置。藉此，該交易資訊可避免被該賣方所竄改。

根據本發明之資訊處理系統所執行的資訊處理流程，



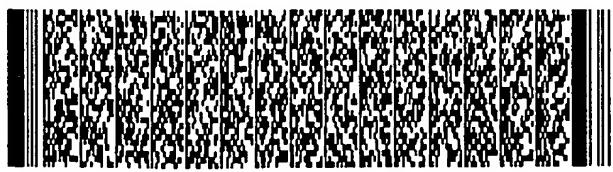
五、發明說明 (4)

首先，於該第三方處，基於該第一資訊對該第二資訊加密以產生一加密的第二資訊。接著，從該第三方傳送該第一資訊以及該加密的第二資訊至該賣方，並且將該第一資訊以及該加密的第二資訊儲存於該賣方處。隨後，從該賣方接收一要求資訊，該要求資訊係表示對該交易要求做一核對。接著從該賣方取出該第一資訊以及該加密的第二資訊至該第三方。接著，於該第三方處，基於該第一資訊對該加密的第二資訊解密，進而重新獲得該交易資訊。隨後，於該第三方處，根據該重新獲得之交易資訊產生一回應資訊，該回應資訊係回應該要求資訊。接著，傳送該回應資訊至該賣方。

關於本發明之優點與精神可以藉由以下的發明詳述及所附圖式得到進一步的瞭解。

發明之詳細說明

一般在每一筆交易完成後，賣方(商家)皆必須儲存關於該筆已交易完成之資訊，以供作日後自己稽核帳目之用。因此，賣方必須做好交易資訊儲存管理的工作。隨著交易模式日漸複雜，交易過程中，除了買、賣兩方外，甚至會牽涉到代為轉帳、付款、授權的機構，因此，賣方(商家)必須儲存關於該筆已交易完成之資訊，以作為與另一機構做帳目核對之用。為避免不肖商家將所儲存的交易資訊，藉由竄改或變造交易資訊向代付款、轉帳機構進行詐欺，進而讓買方(消費者)的權益蒙受損失。如先前技術



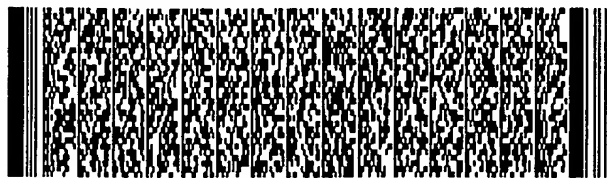
五、發明說明 (5)

著重的，交易資訊在儲存及核對過程中，必須加入加、解密的程序，如此才可做好保全的工作。

本發明係提供一種經由一第三方來管理及保全一交易資訊之系統及方法，該筆交易係於一買方與一賣方之間所達成。不同於先前技術，根據本發明之系統及方法係藉由該受信任的第三方參與該交易資訊的管理及保全。特別地，該交易資訊之管理及保全過程中，關於該買方(消費者)的相關資訊之加、解密工作並非交由該賣方執行，而是交由該第三方來執行。如此賣方(商家)無法獲知買方(消費者)的資訊，即便是不肖的網路商家也就無法竄改或假造交易資料，藉此確實地保護該消費者的權益。以下將詳述本發明之較佳具體實施例，藉以充分解說本發明之特徵、精神以及優點。

請參閱圖一，圖一係為根據本發明之一較佳具體實施例之一資料處理系統40的實施環境示意圖。該資料處理系統40係藉由一第三方10來管理及保全關於一筆交易之一交易資訊。該筆交易係已於一賣方20(如一網路商家)與一買方(消費者)之間達成。如圖一所示，該買方係藉由一上網裝置30與一第三方10做一通訊連結，進而將關於該筆交易之交易資訊傳送至該第三方10。同樣示於圖一，該賣方20與該第三方10做一通訊連結。

如圖一所示，根據本發明之較佳具體實施例之資料處理系統40包含一第一處理裝置42及一第二處理裝置44。該第一處理裝置42係由該第三方10所操控，亦可以設於該第



五、發明說明 (6)

三方10內，如圖一所示。該第二處理裝置44係由該賣方20所操控，亦可以設於該賣方20內，如圖一所示。該第二處理裝置44並且與該第一處理裝置42互相連結。

如圖二A所示，關於該筆交易之交易資訊50包含關於該賣方20之一第一資訊52以及關於該買方之一第二資訊54。該第一處理裝置42係用以基於關於該賣方20之第一資訊來對該關於該買方之第二資訊做加密處理，進而產生如圖二B所示之一加密的第二資訊58。圖二B所示之交易資訊56，即為圖二A所示之尚未經處理的交易資訊50經由該第一處理裝置42處理而得。如圖二A所示，該交易資訊56包含關於該賣方20之第一資訊52以及將第二資訊54加密處理而得之加密的第二資訊58。

上述將交易資訊50先區分為關於賣方20之第一資訊52以及關於買方之第二資訊54，進而對該第二資訊54基於該第一資訊52做加密處理，並且保留該第一資訊52不做處理，其主要目的有二。其一，將關於買方的資訊加密不顯露出來，以便保全關於買方的資訊。其二，保有關於賣方的資訊，讓資訊在管理及儲存過程能作為歸納、索引的依據，並且可考量到作為索引、歸納依據的資訊不會涉及到必須保全的關於賣方之資訊。

需強調的是，該加密的第二資訊58係基於該第一資訊52做加密處理，亦即加密的邏輯中牽涉到該第一資訊52的內容。如此作法，讓該加密的第二資訊58與未經加密處理的第一資訊52之間有著密切的關連性，亦即變更第一資訊



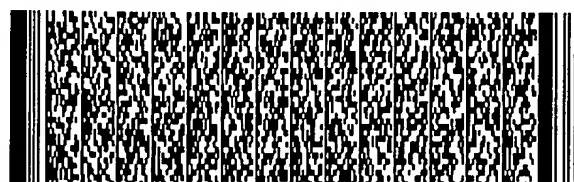
五、發明說明 (7)

52 的內容，之後即無法解密還原。

以下將以該筆交易係透過一信用卡所達成作為說明例，來詳加說明尚未經處理之交易資訊50以及經該第一處理裝置42處理所得的交易資訊56。如圖二A及圖二B所示，關於賣方之第一資訊52可以包含賣方國碼521、賣方序號522等關於賣方的資料。為了後續對於該交易資訊50及交易資訊56能便於管理、避免發生混淆，並且於該交易資訊56後續處理過程能快速指引該筆交易，除了上述關於賣方的詳細資料外，該第一資訊52並且可以包含一用以指引至該筆交易的索引資訊。同樣示於圖二A及圖二B，該索引資訊可以包含交易時間523、發卡行國碼524、發卡行序號525、產品/服務編號526等可供指引至該筆交易的資料，但是該索引資訊的內容並未涉及關於該買方之資訊。

該第一處理裝置42隨後將該第一資訊52以及該加密的第二資訊58傳送至該第二處理裝置44。該第二處理裝置44於接收到該第一資訊52以及該加密的第二資訊58後，即將該第一資訊52以及該加密的第二資訊58合併儲存。

當該賣方20要求對該筆交易做一核對時，該第二處理裝置44即將該第一資訊52以及該加密的第二資訊58回傳至該第一處理裝置42。隨後，當該第一處理裝置42接收到回傳之該第一資訊42以及該加密的第二資訊58時，該第一處理裝置42即基於該第一資訊52對該加密的第二資訊58解密，進而重新獲得該交易資訊。該第一處理裝置42並且根據該重新獲得之交易資訊產生一回應資訊，該回應資訊係



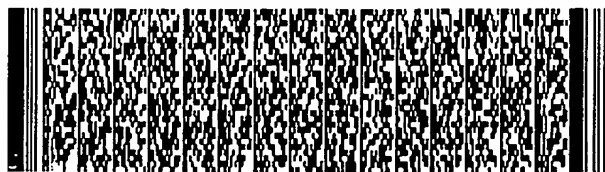
五、發明說明 (8)

回應該賣方20對核對該交易之要求。該第一處理裝置34並且將該回應資訊傳送至該第二處理裝置24。

於一具體實施例中，該回應資訊包含了一顯示關於該交易之一金額的資訊。於另一具體實施例中，該回應資訊包含一用以確認該筆交易之資訊，例如，以簡單的"是"或"否"的訊息來代表確認該筆交易的真、偽。

由以上的說明可以清楚看出，該賣方20始終無法獲得關於該買方的資訊。由於該第一資訊52與該第二資訊54所組成的交易資訊50係為唯一值，一旦該賣方20變更其所儲存的第一資訊52或是加密的第二資訊58，隨後該第一處理裝置42基於變更的第一資訊52來對該加密的第二資訊58解密，或是基於該第一資訊52來對加密並且變更的第二資訊58解密，結果都是獲得一個無效的資訊。藉此，可以明確地保全買方的權益。

以下將詳述應用本發明之較佳具體實施例之資料處理系統40的資訊處理流程。請參閱圖三，首先，執行步驟S60，於該第三方10處，基於該第一資訊52對該第二資訊54加密，進而產生加密的第二資訊58。接著，執行步驟S62，從該第三方10傳送該第一資訊52以及該加密的第二資訊58至該賣方20，並且將該第一資訊52以及該加密的第二資訊58儲存於該賣方20處。接著，執行步驟S64，從該賣方20處接收一要求資訊，該要求資訊係表示要求對該筆交易做一核對。接著，執行步驟S66，從該賣方20取出該第一資訊52以及該加密的第二資訊58，隨即傳送至該第三方

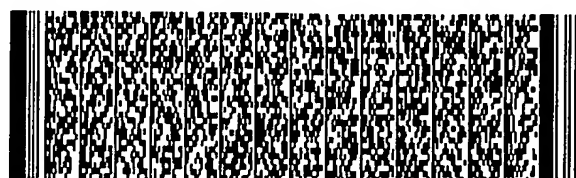


五、發明說明 (9)

10。接著，執行步驟S68，於該第三方10處，基於回傳的第一資訊52對該加密的第二資訊58進行解密，進而重新獲得該交易資訊50。接著，執行步驟S70，於該第三方10處，根據該重新獲得之交易資訊50產生一回應資訊，該回應資訊係回應該要求資訊。接著，執行步驟S72，傳送該回應資訊至該賣方20。

由以上的說明例可看出，藉由本發明之經由第三方管理及保全交易資訊之系統及方法，可以對關於每筆交易之交易資訊做到妥善的管理以及保全，使得買、賣雙方以及代為轉帳或授權等機構的權益都不會受損。因此，根據本發明之系統及方法，能讓透過網路達成交易的買、賣雙方以其他涉及交易過程之機構彼此之間的互信機制更為完備，促使透過網路達成交易的模式更為蓬勃發展，對人類生活的進化將有相當的助益。

藉由以上較佳具體實施例之詳述，係希望能更加清楚描述本發明之特徵與精神，而並非以上述所揭露的較佳具體實施例來對本發明之範疇加以限制。相反地，其目的是希望能涵蓋各種改變及具相等性的安排於本發明所欲申請之專利範圍的範疇內。



圖式簡單說明

圖一係揭露根據本發明之一較佳具體實施例之資料處理系統40以及其實施環境示意圖。

圖二A係繪示一尚未經處理之交易資訊50，該交易資訊50包含關於賣方的第一資訊52以及關於買方的第二資訊54。

圖二B係繪示圖二A之交易資訊50經處理所得的交易資訊56，該交易資訊56包含關於賣方的第一資訊52以及將第二資訊54加密處理而得之加密的第二資訊58。

圖三係本發明之較佳具體實施例之實施步驟流程圖。



六、申請專利範圍

1、一種資料處理系統，該資料處理系統係用以經由一第三方來管理及保全關於一交易之一交易資訊，該交易係於一買方與一賣方之間達成，該交易資訊包含關於該賣方之一第一資訊以及關於該買方之一第二資訊，該系統包含：

一第一處理裝置，該第一處理裝置係由該第三方所操控，該第一處理裝置係用以基於該第一資訊對該第二資訊加密以產生一加密的第二資訊，並且將該第一資訊以及該加密的第二資訊傳送出去；

一第二處理裝置，該第二處理裝置係由該賣方所操控，該第二處理裝置並且與該第一處理裝置相連結，該第二處理裝置係用以儲存從該第一處理裝置傳送來之該第一資訊以及該加密的第二資訊，並且當該賣方要求對該交易做一核對時，該第二處理裝置係用以將該第一資訊以及該加密的第二資訊回傳至該第一處理裝置，其中當該第一處理裝置接收到回傳之該第一資訊以及該加密的第二資訊時，該第一處理裝置係基於該第一資訊對該加密的第二資訊解密進而重新獲得該交易資訊，該第一處理裝置並且根據該重新獲得之交易資訊產生一回應資訊，該回應資訊係回應該賣方對核對該交易之要求，該第一處理裝置並且將該回應資訊傳送至該第二處理裝置；



六、申請專利範圍

藉此，該交易資訊係避免被該賣方所竄改。

2、如申請專利範圍第1項所述之資料處理系統，其中該回應資訊包含一用以確認該交易之資訊。

3、如申請專利範圍第1項所述之資料處理系統，其中該回應資訊包含一顯示關於該交易之一金額的資訊。

4、如申請專利範圍第1項所述之資料處理系統，其中該第一資訊並且包含一索引資訊，該索引資訊係用以指引至該交易。

5、一種資料處理方法，該資料處理方法係用以經由一第三方來管理及保全關於一交易之一交易資訊，該交易係於一買方與一賣方之間達成，該交易資訊包含關於該賣方之一第一資訊以及關於該買方之一第二資訊，該方法包含下列步驟：

(a) 於該第三方處，基於該第一資訊對該第二資訊加密以產生一加密的第二資訊；

(b) 從該第三方傳送該第一資訊以及該加密的第二資訊至該賣方，並且將該第一資訊以及該加密的第二資訊儲



六、申請專利範圍

存於該賣方處；

(c) 從該賣方接收一要求資訊，該要求資訊係表示對該交易要求做一核對；

(d) 從該賣方取出該第一資訊以及該加密的第二資訊至該第三方；

(e) 於該第三方處，基於該第一資訊對該加密的第二資訊解密，進而重新獲得該交易資訊；

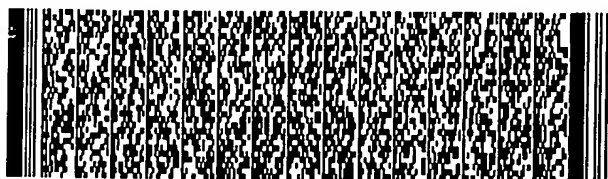
(f) 於該第三方處，根據該重新獲得之交易資訊產生一回應資訊，該回應資訊係回應該要求資訊；

(g) 傳送該回應資訊至該賣方；

藉此，該交易資訊係避免被該賣方所竄改。

6、如申請專利範圍第5項之資料處理方法，其中該回應資訊包含一用以確認該交易之資訊。

7、如申請專利範圍第5項之資料處理方法，其中該回應資訊包含一顯示關於該交易之一金額的資訊。

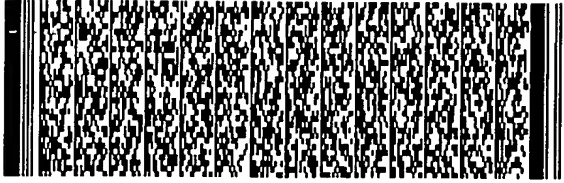


六、申請專利範圍

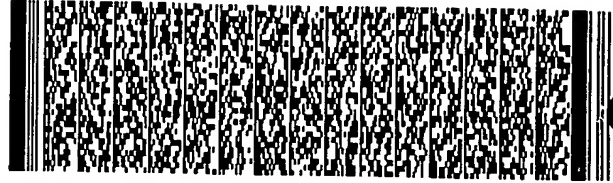
8、如申請專利範圍第5項之資料處理方法，其中該第一資訊並且包含一索引資訊，該索引資訊係用以指引至該交易。



第 1/18 頁



第 2/18 頁



第 3/18 頁



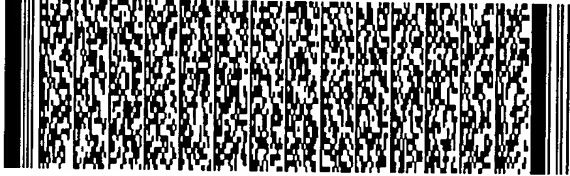
第 5/18 頁



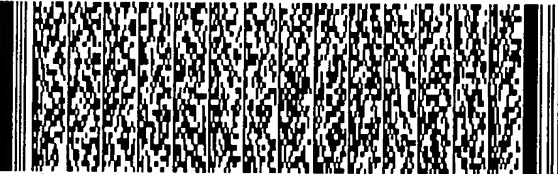
第 5/18 頁



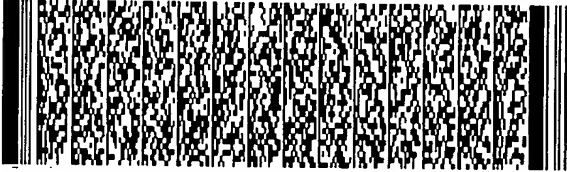
第 6/18 頁



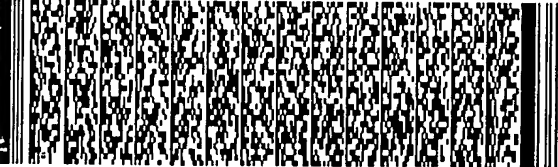
第 6/18 頁



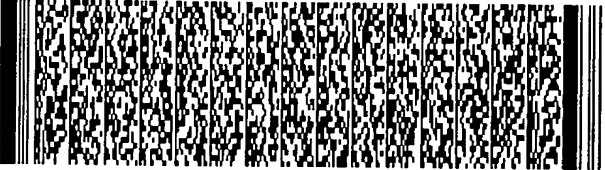
第 7/18 頁



第 7/18 頁



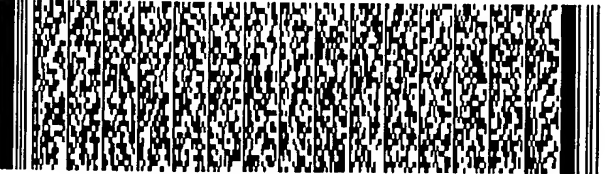
第 8/18 頁



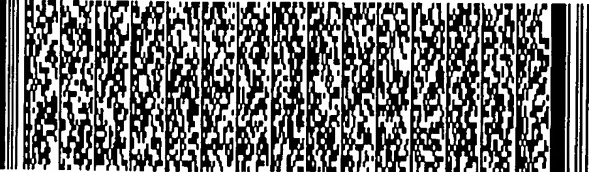
第 8/18 頁



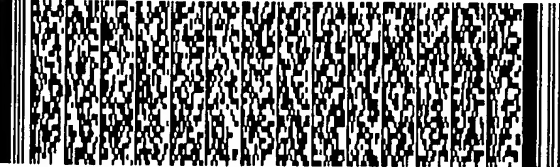
第 9/18 頁



第 9/18 頁



第 10/18 頁



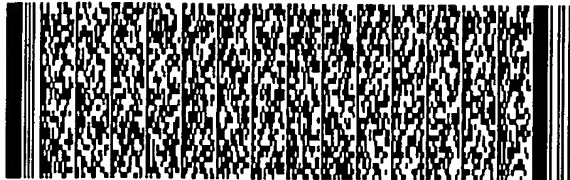
第 10/18 頁



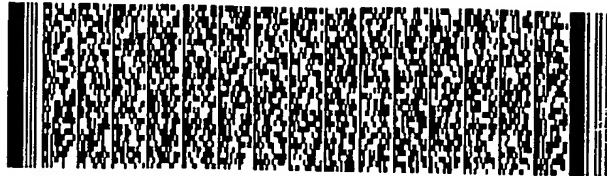
第 11/18 頁



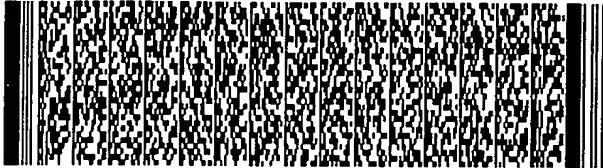
第 11/18 頁



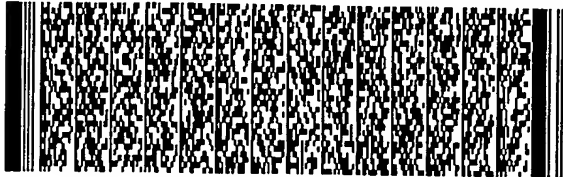
第 12/18 頁



第 12/18 頁



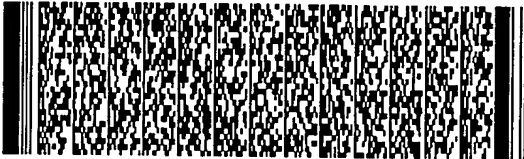
第 13/18 頁



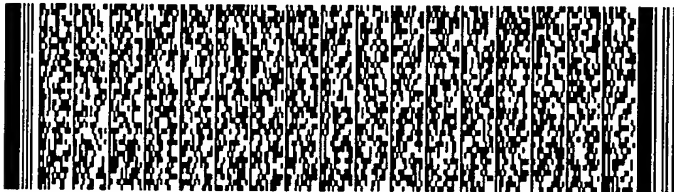
第 13/18 頁



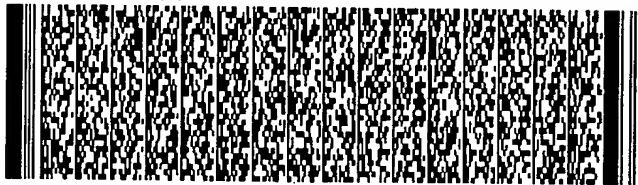
第 14/18 頁



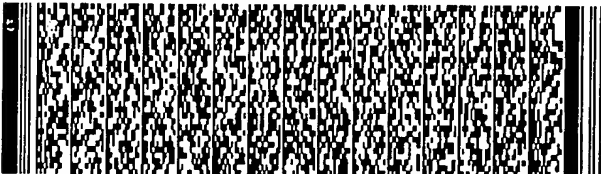
第 15/18 頁



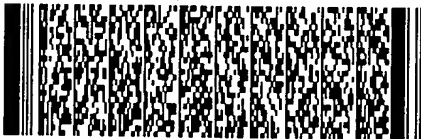
第 16/18 頁

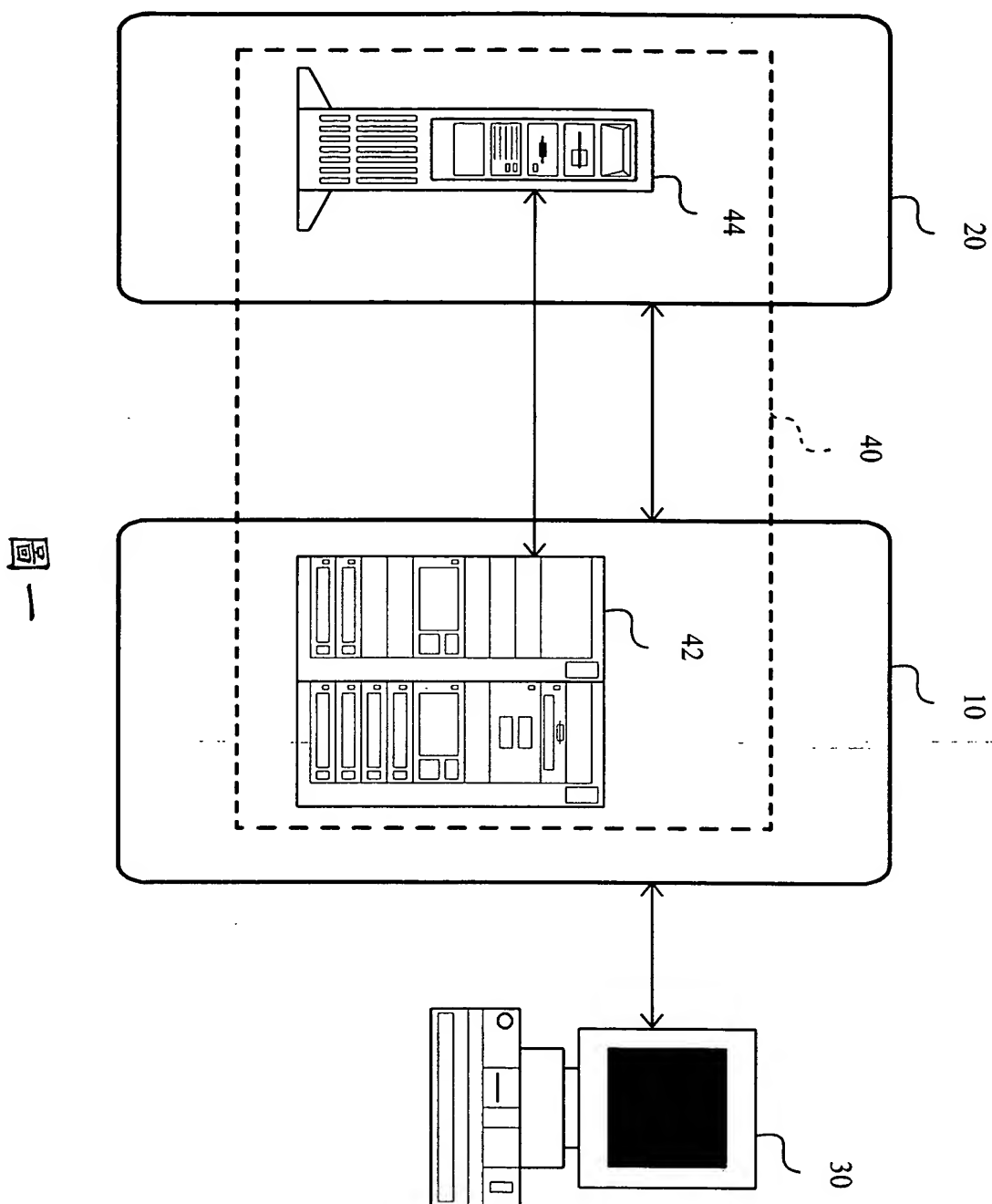


第 17/18 頁

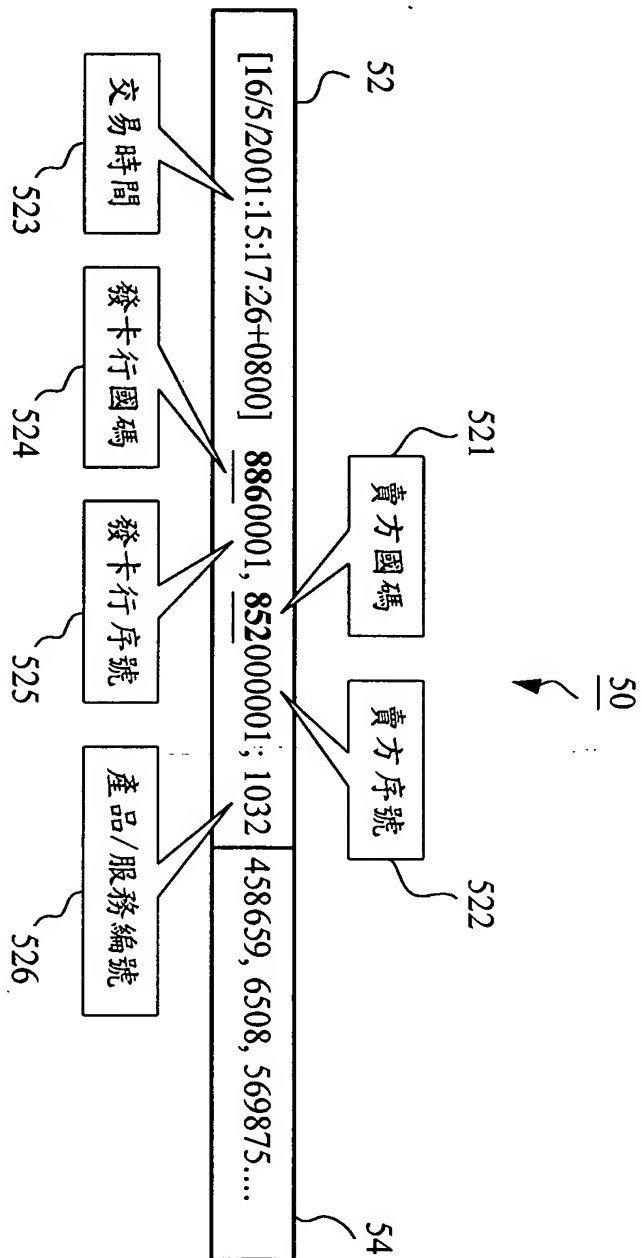


第 18/18 頁

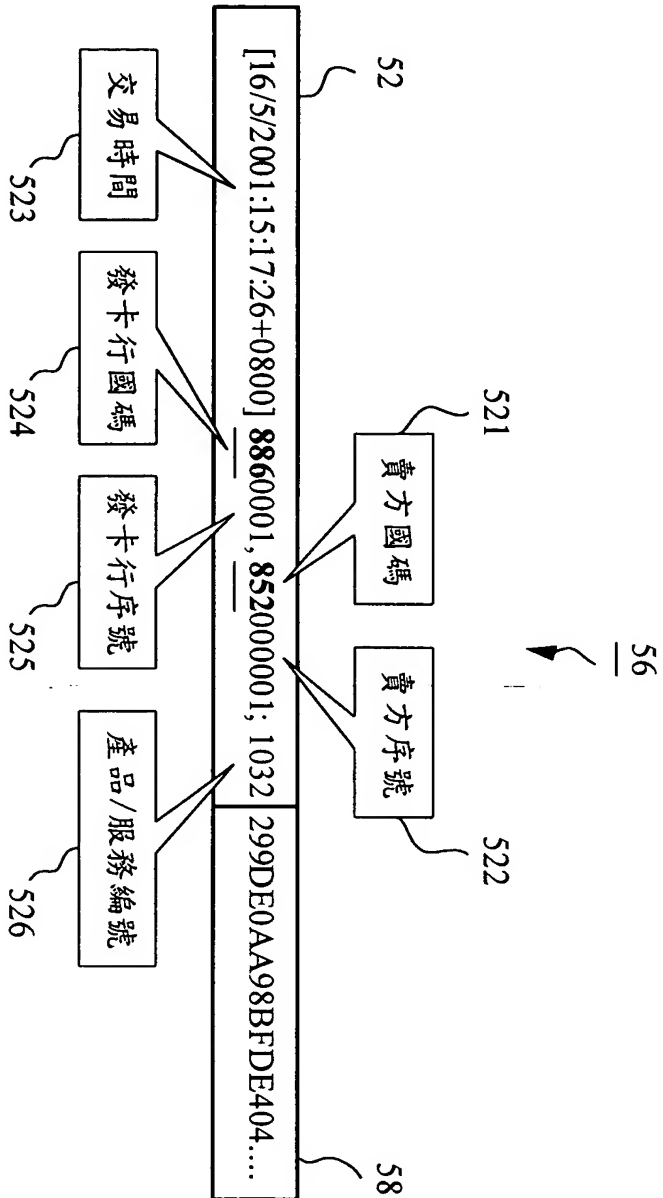




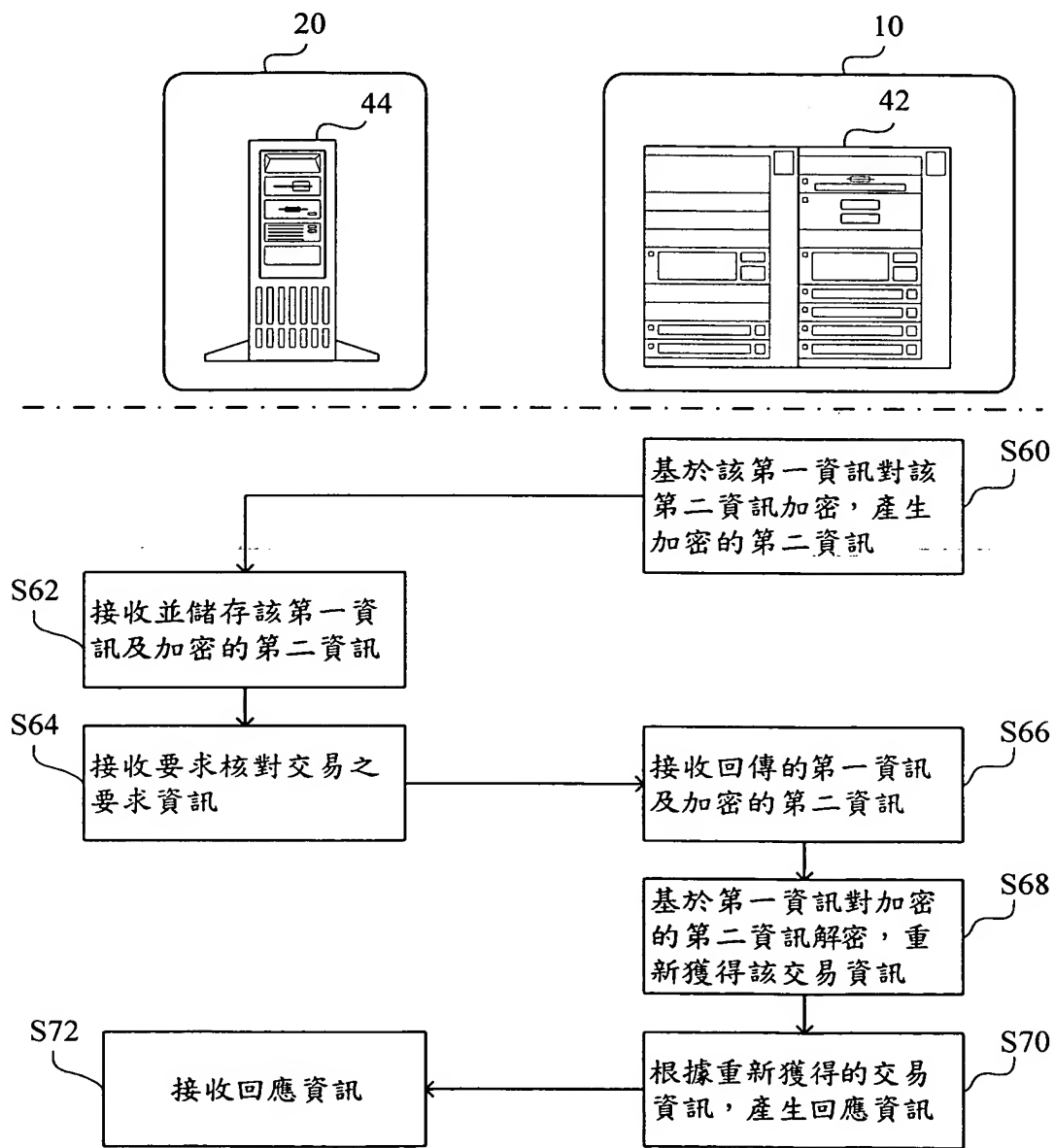
圖一



圖二A



圖二B



圖三